**DEPARTMENT OF THE NAVY**

COMMANDER NAVAL RESERVE FORCE
4400 DAUPHINE STREET
NEW ORLEANS, LOUISIANA 70146-5046

COMNAVRESFORINST 5239.3
N64

31 JAN 2002

COMNAVRESFOR INSTRUCTION 5239.3

Subj: NAVAL RESERVE INFORMATION ASSURANCE (IA) PROGRAM

Ref: (a) Computer Security Act of 1987 (Public Law 100-235)
(b) OMB Circular No. A-130 of 8 Feb 96
(c) DoDD 5200.28 of 21 Mar 88
(d) DoDI 5215.2 of 2 Sep 86
(e) SECNAVINST 5239.3
(f) OPNAVINST 5239.1B
(g) SECNAVINST 5000.2B
(h) SECNAVINST 5510.36
(i) DoD 5500.7-R of 30 Aug 93
(j) DoDI 5200.40 of 30 Dec 97
(k) SECNAVINST 5214.2B
(l) CNO Washington DC 231302Z MAR 00 (NAVADMIN 064/00)
(m) SECNAVINST 5720.44A
(n) NAVSO P-5239-04
(o) OPNAVINST C5510.93E (NOTAL)
(p) OPNAVNOTE C5510 of 14 Apr 94 (NOTAL)

Encl: (1) Definition of Terms
(2) Minimum Program Requirements
(3) Information System (IS) Incident and Vulnerability Report Format

1. Purpose

a. To provide a command Information System (IS) security policy and to establish and implement the Commander, Naval Reserve Force (COMNAVRESFOR) IA Program to meet the requirements of references (a) through (p).

b. To define the organizational structure of COMNAVRESFOR's IA Program.

c. To issue policies and guidelines necessary for consistent and effective implementation throughout the Naval Reserve.

d. To apply basic policy and principles of security as they relate to Information Technology (IT) and ISs associated with, or connected to, the Naval Reserve Network (NAVRESNET) and Naval Reserve owned web sites.

2. Cancellation. COMNAVRESFORINST 5239.1A

3. Definitions. Enclosure (1) of this instruction defines relevant terms.

4. Objective

a. To ensure information processed, stored, or transmitted by COMNAVRESFOR ISs is adequately protected with respect to confidentiality, integrity, availability, privacy, and nonrepudiation.

b. To implement programs which mandate the certification and accreditation of ISs under COMNAVRESFOR cognizance.

c. To require a Life Cycle Management (LCM) approach to implementing IA requirements.

d. To establish standardized IA training within COMNAVRESFOR.

e. To ensure countermeasures are provided. The collection of countermeasures shall include physical, personnel, communications, emanations, hardware, software, data security elements, and administrative and operational procedures. They shall protect against such events as material hazards, fire, misuse, espionage, sabotage, malicious acts, or accidental/inadvertent damage.

5. Scope. COMNAVRESFOR is responsible for ensuring compliance with the Department of the Navy (DON) IA Program identified in references (e) and (f). The procedures and principles presented in these guidelines apply to all COMNAVRESFOR military and civilian employees (including government contractors) and all IT assets within the COMNAVRESFOR claimancy. Minimum program requirements are delineated in enclosure (2) of this instruction.

6. Background. References (a) through (f) direct each agency to implement and maintain an IA program to assure adequate security is provided for all information collected, processed, transmitted, stored, or disseminated in general support systems and major applications. Former COMNAVRESFOR directives did not contain up-to-date guidance for the protection of Local Area Networks or Wide Area Networks. COMNAVRESFOR recognizes the urgent need to integrate all available security capabilities into a unified system-oriented engineering approach to provide responsive, cost effective security measures for Reserve Force ISs.

7. Policy. Ultimate responsibility for security of the NAVRESNET and all COMNAVRESFOR ISs rests with the Designated Approving Authorities (DAAs). COMNAVRESFOR (N6) has been designated as the DAA for the NAVRESNET. Each application and local IS shall have a DAA designated in writing and will normally be the facility or hardware unit Commanding Officer (CO). All subordinate COs are responsible for ensuring compliance with this instruction.

a. Fundamental IA Policy

(1) Accreditation. IT, network, and computer resources will be accredited by the appropriate DAA using reference (j), DoD Information Technology Security Certification and Accreditation Process (commonly known as DITSCAP).

(2) LCM. Action shall be taken throughout the life cycle of all IT, network, or computer resources to ensure compliance with security policies.

(3) Risk Management. DAAs will ensure that a continuing risk management process is in effect to minimize the potential for unauthorized disclosure of sensitive information, modification or destruction of assets, or denial of service. Risk management shall be applied throughout the life cycle of all IT, network, and computer resources.

(4) Contingency Planning. Contingency plans shall be developed and tested to the maximum extent feasible. This testing will ensure the plans function in a reliable manner and that adequate backup functions are in place to ensure critical service is maintained. Plans shall be tested before accreditation. If the plan cannot be tested under realistic conditions, the DAA shall issue an Interim Authority to Operate (IATO) pending completion of testing.

(5) User Access. IT, network, or other computer resources will follow the "least privilege" principle (per reference (a)) so that each user is granted access to only the information to which the user is authorized. This is done by virtue of security clearance and formal access approval to resources necessary to perform assigned functions. In the absence of a specific positive access grant, user access shall default to no access.

(6) Security Implementation. All COMNAVRESFOR resources that process or handle classified or sensitive unclassified information shall implement Controlled Access Protection (Class C2) functionality.

(7) Emanations Security (EMSEC or TEMPEST). TEMPEST certified equipment is not required for CONUS commands (including Alaska and Hawaii) processing General Services secret or below and Special Category confidential and below. The requirement for TEMPEST Vulnerability Assessment Requests was canceled by reference (p).

(8) Interoperability. Security measures for systems connected to other systems via networks or long-haul communications will employ technological security solutions that provide for interoperability to the maximum extent feasible.

(9) Accessibility. The echelon II command Information System Security Manager (ISSM) functions as the focal point in matters concerning IA and will have direct access to COMNAVRESFOR, COMNAVRESFOR Chief of Staff, COMNAVRESFOR Deputy Chiefs of Staff, and the DAA. ISSMs at lower echelons shall have direct access to their activity CO or officer in charge on matters related to IA.

8. Responsibilities

a. COMNAVRESFOR is the DAA for NAVRESNET and all COMNAVRESFOR ISs. The DAA is the official with authority to accredit or grant an IATO for all ISs that fall under his/her cognizance. The DAA shall:

(1) Ensure the development of an IA program to provide adequate security to protect all ISs and ensure compliance with the DON Security program.

(2) Per references (f) and (n), appoint in writing:

(a) An Information Assurance Officer (IAO) to oversee the IA program and provide IA guidance to subordinate commands.

(b) An ISSM to oversee and implement the IA program within the claimancy. This may be, but need not be, the same individual as the IAO.

(c) An Information Systems Security Officer (ISSO) to assist the ISSM in all IA matters.

(d) A Network Security Officer (NSO) to act as the focal point for all network matters.

(3) Ensure contract specifications for IS equipment, software, maintenance, and professional services satisfy IA requirements.

(4) Ensure security requirements are included in LCM documentation.

Security will be built into systems, whenever possible, to prohibit users from accessing restricted and/or need-to-know only information.

b. The COMNAVRESFOR staff ISSM performs his or her duties per reference (n). The ISSM shall:

(1) Ensure the development of an IA program to provide adequate security to protect all ISs and ensure compliance with the DON Security program.

(2) Provide policy, coordination, and management oversight of the overall COMNAVRESFOR IA program including unclassified data, program development, implementation, control, planning, programming, and budgeting consistent with national goals and policies established by the Department of Defense (DoD) and DON.

(3) Serve as COMNAVRESFOR focal point on all matters relating to the DON IA program.

(a) Coordinate, consolidate, present, and defend Program Objective Memoranda (POM) inputs.

(b) Provide for COMNAVRESFOR's compliance with the DoD IA Vulnerability Reporting Program.

(c) Advise Naval Network Operations Command, Space and Naval Warfare Systems Command, and others of computer security and/or TEMPEST matters of general DON interest for publication, as appropriate. Emphasis should be placed on reporting significant security difficulties and their correction.

(4) Draft instructions relating to IA.

(5) Coordinate procedures for physical protection of IS resources throughout the command and prepare instructions relating to these procedures.

(6) Provide guidance to all commands and echelons within COMNAVRESFOR with respect to formulating and implementing adequate IA policy, security plans, procedures, risk assessments, and contingency plans.

(7) Develop and conduct command IA awareness and training courses.

(8) Make necessary reports to Chief of Naval Operations (CNO), DoD, and other IA managers.

(9) Serve as senior advisor to the Contracting Officer's Representative (COR) and/or a designated contract task monitor.

(10) Design and coordinate security procedures for new systems.

(11) Review current and planned ISs and procedures to ensure that effective security integrity is included and maintained.

c. The NSO, appointed in writing by the DAA, shall:

(1) Oversee, manage, control, and report to the ISSM on IA matters relative to the NAVRESNET.

(2) Conduct periodic IA surveys of the NAVRESNET.

(3) Coordinate with the ISSM in performing risk assessments for the NAVRESNET.

(4) Maintain a registry of authorized NAVRESNET users.

(5) Not be the same person as the ISSM or ISSO.

d. The COMNAVRESFOR staff ISSO, appointed in writing by the DAA, shall:

(1) Maintain a complete IS equipment and software inventory consistent with standards and procedures established by the ISSM.

(2) Conduct and report on periodic (minimum annually) audits of IS devices to ensure that only authorized software is being used and that there is no unauthorized software duplication, distribution, or use (piracy) occurring within the area of responsibility.

(3) Conduct and/or assist the ISSM in conducting periodic IS Security Surveys and Risk Assessments.

(4) Enforce all security requirements implemented by the ISSM for remote terminal areas and stand-alone devices.

(5) Ensure that all countermeasures required to protect data, devices, and information are in place.

(6) Provide IS Incident and Vulnerability reports to the ISSM.

(7) Provide support and report to the ISSM on all IA matters.

(8) Report security violations/incidents using enclosure (3) of this instruction.

e. Each echelon III, IV, and V command shall:

(1) Ensure all ISs or networks used by the command are individually and collectively accredited by the site DAA, or by the appropriate DAA in the case of IS services centrally procured or provided by another command. While it is expected that a certification agent, ISSM, or ISSO will assist the commander in this effort, accreditation is considered a command responsibility.

(2) Develop and manage a program to implement DoD, Secretary of the Navy, DON, CNO, and COMNAVRESFOR IA policy.

(3) Coordinate with COMNAVRESFOR and the chain of command, as appropriate.

(4) Appoint, in writing, an ISSM or ISSO to act as the focal point for all IA matters. Where management and administrative functions have been consolidated within a Navy organization, the higher-level organization head may designate a single ISSM to manage the IA program for the entire organization, and subordinate ISSMs need not be appointed. Echelon III commands shall provide a copy of all designation letters to the COMNAVRESFOR IAO.

(5) Provide program management recommendations to the command ISSM, as appropriate.

(6) Provide support to COMNAVRESFOR teams performing computer security inspections and audits, as requested.

(7) Tailor accreditation guidelines to meet their unique requirements.

(8) Provide LCM technical support.

(9) Make POM recommendations to COMNAVRESFOR (N6) ISSM, as appropriate.

(10) Provide security training expertise or assistance, as necessary.

(11) Provide IS Incident and Vulnerability reports to the COMNAVRESFOR (N6) ISSM.

(12) Ensure that accreditation requests for systems and networks processing National Cryptologic, SCI/Intelligence and SIOP-ESI data are forwarded via the chain of command to Commander, Naval Security Group or Commander, Naval Intelligence Command, as appropriate, for forwarding to higher authority DAA.

(13) Conduct periodic (minimum annually) audits of IS devices to ensure that only authorized software is being used and that there is no unauthorized software duplication, distribution, or use occurring within their area of responsibility.

(14) Due to the dynamic, rapid deployment, and impact to IA caused by technological advancement, highly recommend that commands view www.navres.navy.mil/navresfor on a routine basis for new developments and changes to the COMNAVRESFOR IA posture and policies. For higher guidance, go to www.infosec.navy.mil.

9. Action. Echelon III and subordinate commands will implement this guidance within their command.

10. Reports. COMNAVRESFOR report symbol 5239-3, IS Incident and Vulnerability Report, cited in paragraphs 8d(6) and 8e(11) above, is assigned to this report and will remain in effect for 3 years from the issue date of this instruction.

R. L. PAGE
Chief of Staff

Distribution: (COMNAVRESFORINST 5218.2C)
List B (less 23C)
C1
C2 (C61D only)
D
E6 (FJA8 only)

DEFINITION OF TERMS

1. ACCREDITATION: A formal declaration by the DAA that an IS, network, or computer resource is approved to operate in a particular security mode using a prescribed set of safeguards. Accreditation is the official management authorization for operation and is based on the certification process as well as other management considerations. The accreditation statement affixes security responsibility with the DAA and shows that due care has been taken for security.

2. ASSET: Any software, data, or hardware resource within an IS or network.

3. CERTIFICATION: The technical evaluation made as part of and in support of the accreditation process, that establishes the extent to which a particular computer system or network design and implementation meets a prespecified set of security requirements.

4. COMPROMISING EMANATIONS: Unintentional relay of intelligence-bearing signals that, if intercepted and analyzed, disclose the classified information transmitted, received, handled, or otherwise processed by any information processing equipment.

5. CONTINGENCY PLAN: A plan for emergency response, backup operations, and post disaster recovery maintained by an activity as a part of its Information Systems Security (INFOSEC) program. The plan is a comprehensive statement of all the planned actions to be taken before, during and after a disaster or emergency condition. This statement shall include documented, tested procedures to ensure the availability of critical computer resources and facilitate maintaining the continuity of IS operations in an emergency situation.

6. COUNTERMEASURE: Any action, device, procedure, technique, or other measure that reduces the vulnerability of a system.

7. DATA INTEGRITY: The state that exists when data is unchanged from its source and has not been subjected to accidental or malicious modification, unauthorized disclosure, or destruction.

8. DENIAL OF SERVICE: Action or actions that result in the inability of an IS or any essential part to perform its designated mission, either by loss or degradation of operational capability.

9. DESIGNATED APPROVING AUTHORITY (DAA): Official with the authority to formally assume responsibility for operating an IS or network at an acceptable level of risk.

10. DoD INFORMATION TECHNOLOGY SECURITY CERTIFICATION And ACCREDITATION PROCESS (DITSCAP): The standard DoD approach for identifying information security requirements, providing security solutions, and managing information system security activities.

11. EMBEDDED SYSTEM: A system that performs or controls a function either in whole or in part, as an integral element of a larger system or subsystem.

12. INFORMATION ASSURANCE (IA): Information operations that protect and defend information and ISs by ensuring their availability, integrity, authentication, confidentiality, and nonrepudiation. This includes providing

for restoration of information systems by incorporating protection, detection, and reaction capabilities.

13. INFORMATION SYSTEM (IS): An assembly of computer hardware, software, and/or firmware configured to collect, create, communicate, compute, disseminate, process, store and/or control data or information.

14. INFORMATION SYSTEMS SECURITY (INFOSEC): Measures to protect against unauthorized (accidental or intentional) disclosure, modification, or destruction of ISs, networks, and computer resources or denial of service to process data. It includes consideration of all hardware and software functions, characteristics, and/or features; operational procedures, accountability procedures, and access controls at the central computer facility, remote computer and terminal facilities; management constraints; physical structures and devices; and personnel and communication controls needed to provide an acceptable level of risk for the IS or network and data contained therein.

15. INFORMATION SYSTEMS SECURITY MANAGER (ISSM): The person responsible to the DAA who ensures that an IS is approved, operated, and maintained under the System Security Authorization Agreement.

16. INFORMATION SYSTEMS SECURITY OFFICER (ISSO): The person responsible to the ISSM for the day-to-day operation of an IS or network.

17. INTELLIGENCE: Intelligence refers to foreign intelligence and counter-intelligence involving sensitive sources or methods. Intelligence also includes Sensitive Compartmented Information (SCI) and all information that is (or should be) marked WARNING NOTICE - INTELLIGENCE SOURCES AND METHODS INVOLVED.

18. NEED-TO-KNOW: A determination made in the interest of United States national security by the custodian of classified or sensitive unclassified information, that a prospective recipient has a requirement for access to, knowledge of, or possession of the information to perform official tasks or services.

19. NETWORK: The interconnection of two or more independent IS components that provides for the transfer or sharing of computer system assets. It is composed of a communications medium and all components attached to that medium whose responsibility is the transfer of information. Such components may include ISs packet switches, telecommunications controllers, key distribution centers and technical control devices.

20. RESEARCH, DEVELOPMENT AND ACQUISITION PROCESS ACQUIRED - MISSION CRITICAL COMPUTER RESOURCES: Includes computer resources acquired under research, development, and acquisition procedures for use as integral parts of weapons; command and control; communications; intelligence; and other tactical or strategic systems aboard ships, aircraft, shore facilities, and their support systems.

21. RISK: A combination of the likelihood a threat shall occur, the likelihood a threat occurrence shall result in an adverse impact, and the severity of the resulting adverse impact.

22. RISK ASSESSMENT: An analysis of computer system and network assets, vulnerabilities, and threats to determine the security requirements which must be satisfied to ensure the system can be operated at an acceptable level of risk.

23. RISK MANAGEMENT: A process through which undesirable events can be identified, measured, controlled, and prevented so as to effectively minimize their impact or frequency of occurrence. The fundamental element of risk management is the identification of the security posture; i.e., the characteristics of the functional environment from a security perspective. Risk management identifies impact of events on the security posture and determines whether or not such impact is acceptable and, if not acceptable, provides for corrective action. Risk assessment, Security Test and Evaluation (ST&E) and contingency planning are parts of the risk management process.

24. SAFEGUARDS: Protective measures and controls prescribed to meet the security requirements specified for an IS, network, or computer resource. Those safeguards may include, but are not necessarily limited to, hardware and software security features, operational procedures, accountability procedures, access and distribution controls, management constraints, personnel security and physical structures, areas, and devices.

25. SENSITIVE COMPARTMENTED INFORMATION (SCI): Information and material requiring special controls for restricted handling within compartmented intelligence systems and for which compartmentation is established.

26. SENSITIVE INFORMATION: See Sensitive Unclassified Information.

27. SENSITIVE UNCLASSIFIED INFORMATION: Any information the loss, misuse, or unauthorized access to or modification of which could adversely affect the United States national interest, the conduct of Department of the Navy programs or the privacy of Department of the Navy personnel (e.g., Freedom of Information Act exempt information).

28. SIOP-ESI: An acronym for Single Integrated Operational Plan Extremely Sensitive Information; a DoD Special Access program.

29. SYSTEM SECURITY AUTHORIZATION AGREEMENT (SSAA): A formal agreement among the DAA(s), the Certification Authority, the IT system user representative, and the program manager. It is used to guide actions, document decisions, specify security requirements, document certification tailoring and level-of-effort, identify potential solutions, and maintain operational systems security.

30. TELECOMMUNICATIONS: Any transmission, emission, or reception of signs, signals, writing, images, sounds, or information of any nature, by wire, radio, visual, or other electromagnetic systems.

31. TEMPEST: An unclassified short name referring to investigations and studies of compromising emanations. TEMPEST is a commonly used term for equipment and testing. Terminology is migrating to the use of Emission Security (EMSEC).

32. VIRUS: A parasitic program that replicates itself by attaching to other programs and files intended to carry out unwanted and sometimes damaging operations. Replication usually occurs during copying of files to magnetic media, or during computer-to-computer communications. The code usually contains malicious logic that is triggered by some predetermined event. When triggered, the code then takes a hostile action against host computer systems.

MINIMUM PROGRAM REQUIRMENTS

1. DAAs will take action necessary to ensure that these minimum requirements are satisfied in a cost-effective manner to meet the unique requirements of their area of responsibility:

a. Individual Accountability. Access to IS, network, and other computer resources will be controlled and monitored to ensure each person having access can be identified and held accountable for their actions.

b. Physical Control. IS, network, and other computer resources will be physically protected against damage and unauthorized access.

c. Data Integrity. Each database or collection of data elements in an IS will have an identifiable origin and use. Its use, backup, accessibility, maintenance, movement, and disposition will be governed on the basis of classification, sensitivity, type of data, need-to-know, and other restrictions.

d. Marking. Permanent human-readable output shall be marked to accurately reflect the sensitivity of the information. The marking may be automated (i.e., the IS has the capability to produce the markings) or may be done manually. Automated markings on output from systems which process or handle classified information must not be relied upon to be accurate unless security features and assurances of the system meet the requirements for a minimum-security class B1.

e. Access. There shall be in place an access control policy for each IS. It shall include features and/or procedures to enforce the access control policy of the information contained within the IS. The identity of each user-authorized access to IS shall be positively established before authorizing access.

f. Network/Communication Links. All communications circuits will be secured per the communications security program (reference (h)). Those handling plain text classified will be installed in an approved protected distribution system. For purposes of accreditation, a network shall be treated as either an interconnection of accredited ISs (which may, themselves, be networks) or as a single distributed system.

g. Accreditation. Each IS, network, or computer resource shall be accredited to operate per a DAA-approved set of security requirements.

h. Risk Management. There shall be in place a risk management program to determine how much protection exists, how much protection is required, and the most economical way of providing needed protection. Risk assessments shall be conducted:

(1) Before design approval.

(2) To support accreditation.

(3) Whenever there is a significant change to the system.

(4) At least once every 3 years.

i. Certification. Systems developers shall certify to the users and the DAA that the system's security requirements have been met and specify any constraints on the system or its environment necessary to maintain the certification.

j. Contingency Planning. Each DON activity will develop and test a contingency plan, addressing both automated and manual backup systems, to provide for continuation of its mission during abnormal operating conditions. The contingency plan will be developed, tested, and maintained to ensure continued performance of mission support and mission critical functions. It must be consistent with disaster recovery and continuity of operations plans. Detail and complexity should be consistent with the value and criticality of the systems.

k. Internal Security Mechanisms. After the system becomes operational, software and files providing internal security controls, passwords or audit trails will be safeguarded at the highest level of data contained in the IS, network, or computer resource. Access to internal security mechanisms will be controlled on a strict need-to-know basis.

l. Encryption. Encryption methods, standards, and devices used to protect classified data processed by an IS, network, or computer resource must be approved by National Security Agency.

m. Emanations Security. IS, network, and computer resources shall follow the emanations security (TEMPEST) requirements of references (o) and (p).

n. Privately Owned Resources. Use of privately owned or leased assets to connect to any Navy or Marine Corps Network is not authorized. Privately owned or leased assets shall not be used to process classified data. Privately owned or leased assets include, but are not limited to, personal computers, personal electronic devices, software, IS appliances (routers, hubs, sniffers, etc.), and Public Data Networks.

o. Access Warning. A warning against unauthorized access will be displayed (physically or electronically) on all visual display devices, cathode ray tubes or other input/output devices upon initial connection, log-on, or system start-up of all computer systems (direct or remote access).

p. Security Levels. All COMNAVRESFOR IS, networks, or other computer resources must implement at least C2 level functionality per reference (c), provided feasible security technology is available. Hardware and software security requirements of COMNAVRESFOR computer resources should be determined per reference (c).

q. Security Training and Awareness. There shall be in place a security training and awareness program to provide training for the security needs of all persons accessing an IS, network, or computer resource. The program shall ensure that all persons responsible for an IS, network, computer resource, and/or the information contained therein and all persons who must access them are aware of proper operational and security-related procedures and risks. In addition, periodic security awareness training will be provided to all personnel. At a minimum, the program shall meet requirements of reference (a).

r. Operational Data. No classified or sensitive unclassified data shall be introduced into an IS, network, or computer resource without first identifying its classification or sensitivity. Approval shall be obtained from the ISSM where appropriate.

s. Communications Security. All COMNAVRESFOR activities will establish measures designed to deny unauthorized persons information of value that might be derived from the possession, study or interpretation of telecommunications. The measures include, but are not limited to, the following:

(1) Communication Links. Transmission and communication lines and links which provide secure communication between components of a DON IS authorized to process classified data will be secured in a manner appropriate to the highest classification of the material transmitted through such lines or links.

(2) Interface with Communications Security. A Naval Reserve activity that operates an IS requiring communication support from telecommunications networks will follow applicable Navy communications directives for the handling of classified material. The security measures will be agreed to and implemented before connecting to the communication network.

t. Removable Media. Several factors should be taken into consideration when evaluating the need for removable media. These factors include physical security, classification level, and sensitivity. In environments where data loss or compromise is an issue, the use of removable, securable, data storage systems is encouraged. Fixed internal hard disks are to be avoided in systems that use classified applications and an appropriately secure space is not available.

u. Emergency Destruction. The requirement to establish a policy for the destruction of media, networks, and resources in the event of an emergency shall be addressed in the overall risk management and contingency planning programs.

v. Degaussing. Commands processing classified information are encouraged to acquire and use degaussing equipment approved by the National Security Agency.

w. Malicious Code. Special care shall be taken to reduce the risk of introduction of malicious code, such as logic bombs, Trojan horses, trapdoors and viruses, into computer systems.

x. Public-Disclosure. Prior to public disclosure or discussion of specific IS capabilities, limitations or vulnerabilities, all members of COMNAVRESFOR shall comply with chapter 5, reference (m), DON Public Affairs Policy and Regulations.

## INFORMATION SYSTEM (IS) INCIDENT AND VULNERABILITY REPORT FORMAT

Note: Classification Markings/Distribution Statement. (Computer incident and vulnerability reports are normally UNCLASSIFIED. However, they will be classified at least CONFIDENTIAL if classified data was disclosed or the report describes a vulnerability allowing unauthorized access to classified data.)

1. Required Information

a. Report Date

b. Contact

(1) Name

(2) Organization

(3) Mailing Address

(4) Phone Number

(5) Position

c. Hardware/Software

(1) List hardware and system configuration

(2) Software description

(a) Operating system (include release/version number).

(b) Describe any unique attributes - i.e., locally modified special security properties.

2. Summary of the security incident or vulnerability. Provide a description of the nature and effect of the incident or vulnerability in as general terms as possible. (Penetration of the IS by an unauthorized user, i.e., exploitation of a technical vulnerability, introduction of malicious code.)

3. Detailed description of the security incident or vulnerability

a. A scenario that describes specific conditions to demonstrate the weakness or design deficiency. The description should sufficiently describe the conditions so that the vulnerability can be repeated without further information.

b. Describe the specific impact or the effect of the incident or vulnerability in terms of the following:

(1) Denial of service or recovery time (work hours)

(2) Alteration of information

(3) Compromise of data

Indicate the number of systems affected and work hours expended in resolving the incident. Cite specific examples as appropriate.

c. For incidents or vulnerabilities involving commercial products indicate whether or not the affected vendor has been notified.

4. Suggested Solutions

5. Additional Information

a. Systems specifics

(1) Location

(2) Owner

(3) Network connections

(4) Security attributes

b. System use and highest classification of data on system

c. Additional clarifying information